De-Identification and Aggregation Policy

Department	Reference Number	Organizational Scope	ICES Site	IPC Scope
PLO	015-00-00	ICES Network	ICES Network	All Acts
Original Date (YYYY-MM-DD)	**Current Version** (YYYY-MM-DD)	**Review Frequency**	**Next Review** (Month YYYY)	**Supersedes** (if applicable)
September 2022	2025-07-30	Triennial	July 2028	PO.015
Authority (Title)	Chief Privacy and Legal Officer			
Policy Owner (Title)	Director, Privacy and Legal Office			
Required Reviewers (Titles)	Senior Director, Research, Data and Financial Services			
	Director, Data Quality & Information Management			

Please refer to the **glossary** for bolded terms and their definitions.

Provisions highlighted in grey are not yet in effect and are subject to review and approval by the Information and Privacy Commissioner.

1.0 PURPOSE

1.1 The purpose of this policy is to:

1.1.1 Set out ICES' position with respect to **De-Identification** and **Aggregation** of **Personal Health Information ("PHI")** and **Personal Information ("PI").**

1.1.2 Set out ICES' policy on **Re-Identification**.

1.1.3 Establish the accountable roles and responsibilities for De-Identification and Aggregation of PHI/PI.

2.0 SCOPE

2.1 This policy applies to:

2.1.1 All **ICES Agents** involved in the De-Identification and Aggregation process of PHI/PI for **ICES Purposes**.

2.1.2 All ICES Agents involved in the use of **De-Identified Data** – including **Aggregate Data (Summary Output)** and **Publishable Data** - for ICES Purposes.

2.1.3 All ICES Agents involved in **Re-Identification Risk Assessment ("RIRA").**

3.0 ROLES AND RESPONSIBILITIES

3.1 ICES Chief Privacy and Legal Officer ("CPLO") is accountable for ensuring that ICES defines and implements appropriate Procedures to enable ICES to meet the requirements of this Policy.

3.2 ICES Senior Director, for the platform of Research and Data, and the ICES Senior Director, Strategic Partnerships and Digital Services are responsible for ensuring that ICES has Procedures and criteria with respect to the processes and criteria for De-Identified Data.

3.3 ICES **Principal Investigator**, or if the Principal Investigator is not a Full Status ICES Scientist the Responsible ICES Scientist, is responsible for conducting and documenting RIRAs.

3.4 ICES **Staff Scientists** are responsible for conducting and documenting RIRAs for **ICES Projects** completed for ICES **Knowledge Users**.

4.0 DETAILS

4.1 General Principles

4.1.1 The meaning ascribed to De-Identification must:

(a) in relation to the PHI of an individual, be consistent with the definition of "identifying information" set out in subsection 4(2) of the *Personal Health Information Protection Act, 2004* ("*PHIPA*"), the definition of "de-identify" set out in section 2 of PHIPA, and include consideration of context-specific risks such as small cell sizes, which may, particularly in combination with other available information, increase the likelihood of re-identification.

(b) in relation to the PI of an individual, as defined under the *Coroners Act* and the *Children, Youth and Family Services Act* ("**CYFSA**"), be consistent with the definition of "personal information" set out in the *Freedom of Information and Protection of Privacy Act* and include consideration of context-specific risks such as small cell sizes, which may, particularly in combination with other available information, increase the likelihood of re-identification.

4.1.2 ICES will not use or disclose PHI/PI if other information, namely De-Identified Data, will serve the identified purposes instead. PHI/PI must be used or disclosed only where De-Identified Data will not serve the identified purposes.

4.1.3 Aggregate Data (Summary Output) is a type De-Identified Data at ICES that is subject to the following conditions when sharing with members of a **Project Team** who are not ICES Agents, because such Aggregate Data (Summary Data) may contain **ICES Confidential Information** and/or **Third Party Confidential Information**:

(a) Such individuals who are not ICES Agents are identified as ICES **Collaborating Researchers** on the **Privacy Impact Assessment ("PIA")** for the ICES Project; and

(b) Such individuals sign a "Collaborating Researchers Non-Disclosure Agreement" prior to receiving access to the Aggregate Data (Summary Data).

4.1.4 Publishable Data is a type of De-Identified Data that may be shared publicly without additional conditions because it is created once ICES Confidential Information and/or Third Party Confidential Information is removed from Aggregate Data (Summary Output).

4.1.5 Limitations for using and disclosing De-Identified Data are set out below:

Type of De-Identified Data	Access	Disclosure	Cell Size	Risk Clearance
Publishable Data	Can be shared publicly	- Can be included in manuscript submissions for potential ICES Publications - Can be published in Reports	May not contain cell sizes fewer than six	Must be subject to a RIRA
Aggregate Data (Summary Output)	Can be shared with Project Team subject to the restrictions set out in this Policy for ICES Collaborating Researchers	- Cannot be included in manuscript submissions for potential ICES Publications - Cannot be published in Reports	May contain cell sizes fewer than six	Not subject to a RIRA but responsible ICES Agents must ensure there is no reasonable risk of re-identification in the circumstances

4.1.6 The process and criteria for creating and disclosing De-Identified Data is set out in accompanying Procedures subject to this Policy, including the mechanisms implemented to ensure that the recipients of the De-identified Data or Aggregate Data is disclosed will not use it, either alone or with other information, to identify an individual, unless permitted by law.

4.1.7 Publishable Data must be reviewed and assessed by the responsible ICES Agents identified in this Policy prior to disclosure by ICES, including its inclusion in manuscripts submissions or published in Reports, such that the Publishable Data does not:

(a) Contain information that identifies an individual or could foreseeably be used, either alone or with other information, to re-identify an individual;

(b) Contain cell-sizes fewer than six; and

(c) Contain ICES Confidential Information and Third Party Confidential Information.

4.1.8 The RIRA process and criteria for reviewing and sharing Publishable Data, including in manuscripts or Reports, is set out in accompanying Procedures to this Policy.

4.1.9 ICES must continue to explore new tools available or that are being developed to assist in ensuring that the policy and Procedures with respect to De-Identification and Aggregation are based on an assessment of the actual risk of Re-identification.

4.2 Cell Sizes

4.2.1 Any use and disclosure of De-Identified Data must have regard to the restrictions related to cell sizes of fewer than six contained in **Data Sharing Agreements ("DSA"), Section 52.1(1) Agreements**, **Research Agreements**, and written research plans pursuant to which the PHI/PI was collected.

4.3 Re-Identification

4.3.1 ICES Agents are explicitly prohibited from using De-Identified Data (including information in cell-sizes of fewer than six) to identify an individual, including by attempting to decrypt information that is encrypted for the purpose of Re-Identification, or identifying an individual based on unencrypted information and/or prior knowledge.

4.3.2 Prohibitions on Re-Identification, are set out in a variety of ICES' policies, standards, procedures, the **ICES Agent and Confidentiality Agreement ("ICES Agent CA")**, the **Third Party Service Provider Agreement** template, and privacy and security training and awareness material, and are subject to audits in accordance with the *Privacy and Security Audit Policy*.

4.3.3 Notwithstanding the prohibition in section 4.3.1 above, **Data Covenantors** are permitted to re-identify individuals in the circumstances, and subject to the requirements, identified below:

(a) the re-identfiication activity must be permitted by law (e.g., under s.11.2 of *PHIPA*), as approved by the Director, PLO;

(b) the Data Covenantor must be acting in the course of their duties for ICES when engaging in re-identification (e.g., to re-identify coded data to address data quality issues; to convert information back into the identifiable form it was received in, for purposes of certain disclosures, such as data return; to allow ICES and researchers to contact patients for approved purposes); and

(c) the re-identification must be conducted in accordance with ICES' applicable Policies, Procedures and Practices, including the *Cohort Disclosure Procedure*, the *Data Return Procedure*, and the *Secure Collection, Disclosure and Transfer of PHI/PI Procedure*.

4.4 Re-Identification Risk

4.4.1 At ICES, the concept of Re-Identification must take into consideration contextual factors (thoughtful consideration based on a combination of pre-existing and general knowledge) where it could be reasonably foreseeable in the circumstances that such De-Identified Data could be utilized, either alone or with other information, to identify an individual.

4.4.2 In accordance with the *Re-identification Risk Assessment Procedure*, ICES must take a risk-based approach to assessing Re-Identification risk that: (i) addresses small cell-size (less than six) utilizing techniques such as masking, generalization, and suppression; and (iii) sets out the process and criteria for conducting such a risk-based assessment, having regard to evolving industry information security standards and best practices.

4.4.3 If an assessment of Re-Identification concludes that there is a risk where it could be reasonably foreseeable in the circumstances that such De-Identified Data could be utilized, either alone or with other information to identify the individual, such risk is considered a **Re-identification Risk.**

4.4.4 The criteria for assessing the Re-Identification Risk must include:

(a) Who is the intended audience for the De-Identified Data? What background information is it reasonable to expect that the intended audience is known or assumed to have?

(b) Whether other directly identifying information or indirectly identifying information is available to the audience and could be used, together with the De-Identified Data, to **Re-Identify** an individual;

(c) Whether there is a reasonable chance a person or group with prior knowledge will be able to inadvertently Re-identify an individual and whether there is an inherent risk of re-identification in the De-Identified Data; and

(d) Such criteria are hereinafter known as "Re-identification Risk Assessment Criteria".

4.5 Documentation of a RIRA

4.5.1 Each time a RIRA is completed, a corresponding sub-folder of **Risk Cleared Deliverables** must be created in the **Project T: Drive Folder** where Risk Cleared Deliverables must be saved.

4.5.2 For **Non-Appointed ICES Agents ("NAIAs"),** Aggregate Data (Summary Output) must be risk-cleared prior to being shared with the NAIA outside of the **ICES Data Environment**.

5.0 RELATED DOCUMENTATION

5.1 Policies

5.1.1 *Privacy and Security Audit Policy*

5.2 Standards

5.3 Procedures

5.3.1 *Re-Identification Risk Assessment Procedure*

5.3.2 *Data Return Procedure*

5.3.3 *Secure Collection, Disclosure, and Transfer of PHI/PI Procedure*

5.3.4 *Cohort Disclosure Procedure*

5.4 Tools

5.5 Guidelines

6.0 TRAINING AND COMMUNICATION

6.1 Policies, standards, and procedures are available on the **ICES Intranet**.

6.2 This policy and any related standards and/or administrative procedures are communicated to all **ICES Agents** across the **ICES Network** during onboarding and on a yearly basis. Policy awareness is also supported and promoted by the policy's **Owner**.

6.3 Once new policies, standards, and procedures are published to the **ICES Intranet**, they are communicated to **ICES Agents** on the **ICES Intranet** and through ICES' weekly email with the organization's internal updates.

7.0 COMPLIANCE AND ENFORCEMENT

7.1 **ICES Agents** must comply with all applicable policies, standards, and procedures.

7.2 **ICES Agents** must notify a Privacy and/or Security **Subject Matter Expert ("SME")** at the first reasonable opportunity if they breach or believe there has been a breach of ICES' privacy and security policies, standards, or procedures in accordance with applicable policies and standards, including:

7.2.1 *Privacy Incident and Privacy Breach Management Policy*

7.2.2 *Security Incident Management Standard*

7.3 Enforcement of compliance with this policy is the responsibility of the the **ICES Agent** identified as the Authority of this policy.

7.4 All violations of policies, standards, and procedures may be subject to a range of **Disciplinary Actions** in accordance with applicable policies, including:

7.4.1 *Discipline and Corrective Action Policy*

7.4.2 *Termination of Employment Policy*

7.4.3 *Discipline and Corrective Action in Relation to ICES Data Policy*

7.4.4 *Termination or Cessation of Employment or Contractual Relationship in Relation to ICES Data Policy*

7.5 Compliance is subject to audit in accordance with applicable policies, including:

7.5.1 *Privacy and Security Audit Policy*

8.0 EXCEPTIONS

8.1 Any exceptions requested pursuant to this policy must be in accordance with applicable policies, including:

8.1.1 *Ongoing Review of ICES' Policy Suite Policy*

8.1.2 *Change Management and Exceptions Policy*

8.2 Exceptions cannot relieve ICES of its legal requirements, including but not limited to those established under:

8.2.1 *Personal Health Information Protection Act, 2004 ("PHIPA")* and its regulation;

8.2.2 *Coroners Act* and its applicable regulations;

8.2.3 *Child, Youth and Family Services Act, 2017 ("CYFSA")* and its applicable regulations; and

8.2.4 The **IPC Manual, Coroners Addendum,** and **CYFSA Addendum.**

9.0 CHANGE TABLE

Change Date (YYYY-MM-DD)	**Change Notes**
2025-07-30	■ Reviewed for compliance with ICES' obligations as a Prescribed Entity: ○ **IPC Manual:** Policy, Procedures, and Practices with Respect to De-Identification and Aggregation ○ **Coroners Addendum:** Policy, Procedures, and Practices with Respect to De-Identification and Aggregation ○ **CYFSA Addendum:** Policy, Procedures, and Practices with Respect to De-Identification and Aggregation ■ Added content regarding ICES' role as a Prescribed Entity under CYFSA ■ Added additional details regarding Cell Sizes and Re-Identification ■ Revised to reflect updated template and standardized language in Sections 6.0 to 9.0